

# CYBER SECURITY

WHAT IT IS AND WHY WE CARE

John P Zelsnack CISSP/CISM/CRISC/Securty+/ITILv3  
Senior Technical Manager/Cyber Security Engineer  
*General Dynamics* - Advanced Information Systems

# AGENDA

- Who Am I?
- Breaking it down
- Why Do We Care
- Questions



# Who Am I

- I have worked Information Assurance / Cyber Security field for the past 10 years with General Dynamics - Advanced Information Systems in Fairfax Virginia, supporting federal level cyber security activities for National Reconnaissance Office in Chantilly Virginia.
  - A large focus of my responsibilities include: Creation of enterprise governance policies, definition of implementation methods and validation of adherence to / enforcement of policies.
  - I manage a worldwide staff that specifically focuses on testing of security control implementation to satisfy cyber security requirements.
- I have a Bachelor's Degree from Strayer University in Network Security and a Master Degree from Capitol College in Information Assurance.
- I am a member in good standing with the multiple Information Security Certification organizations actively holding the following certifications
  - Certified Information Systems Security Professional (*CISSP*)
  - Certified Information Security Manager (*CISM*)
  - Certified in Risk and Information Systems Control (*CRISC*)
  - Security+ Certified Professional (*Security+*)
  - Information Technology Information Library (*ITIL*)

# BREAKING IT DOWN

- **What Cyber Security Is:**

- Cyber security is the collection of technologies, services, processes and best practices designed to protect networks, computers, applications and data from attack, damage or unauthorized access.
- Also referred to as Computer Security, Information Security, Information Assurance
- It spans multiple Security disciplines to include Physical Security, Personnel Security, Personal Security, Network Security, Information Security, Communications Security, Operations Security and Security Awareness

- **Physical Security:**

- Protection of technology and data from unauthorized physical access. Includes guards, doors, locks, fences, cameras

- **Personnel Security:**

- Review and assessment of people to validate “worthiness” of access (both physical and virtual) to technology and data

- **Personal Security:**

- Protection of the personnel in an organization that are authorized to access the organization, its technology and data



# BREAKING IT DOWN

- **Network Security:**
  - Technology implemented to protect networks from unauthorized access
- **Information Security:**
  - Protection of an organizations information (data) to include the technology that is used to store, process or transmit the information
- **Communications Security:**
  - Protection of an organizations communication media, technology and content.
- **Operations Security:**
  - Protection of the details regarding an organizations capabilities, methods or activities
- **Security Awareness**
  - Ongoing education and training to ensure that personnel are reminded of and trained on Cyber Security principles

# BREAKING IT DOWN

- What Cyber Security Is Not:
  - Cyber security is not a collection of laws and regulations
  - Cyber security is not a one time install of Anti-virus software
  - Cyber security is not someone else's responsibility
- The common denominator across all disciplines comprising Cyber Security is Security
  - It is important for everyone involved to understand what needs to be protected and why as well as where protection needs to be applied





# WHY DO WE CARE

- Cyberspace:
  - Cyberspace is that worldwide environment of computers and the infrastructure that connects them, more commonly referred to as the Internet
  - The growth in number and prevalence of connected devices has created an environment where both people and organizations are constantly exposed to threats
    - Devices are not just the computer sitting on your desk anymore



- Being “connected” is accepted, expected and inherently trusted

# WHY DO WE CARE

- People are inherently the weak link in all aspects of security
  - We all trust that someone or something else is protecting our interests
  - People tend to lack the due diligence to ensure that all aspects of our part of the cyberspace are adequately protected
  - Connected to the internet = exposed and vulnerable
- So – how do we make it better??
- Education and awareness are key to ensure understanding of the issue and support for the resolutions we are here to help define.



QUESTIONS??